IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF PUERTO RICO

BETZAIDA SANTOS-PAGAN, *et al.*,
Plaintiffs,

v.

BAYAMÓN MEDICAL CENTER,
Defendant.

Civil No. 20-1237 (BJM)

OPINION AND ORDER

In this putative class action, plaintiff Betzaida Santos-Pagan ("Santos-Pagan"), individually and on behalf of others similarly situated, alleges that Bayamón Medical Center ("BMC") is liable for unauthorized disclosure of her protected health information ("PHI") and personal identifying information ("PII"). On May 21, 2019, BMC was subject to a ransomware attack affecting the PHI and PII of more than 500,000 current and former patients. Docket No. ("Dkt.") 113 at ¶ 16. Santos-Pagan, a former patient of BMC, brings claims of negligence, breach of implied contract, and breach of the covenant of good faith and fair dealing, respectively, under Puerto Rico law. *Id*. at ¶¶ 84-130. She also seeks relief under the federal Stored Communications Act, 18 U.S.C. §§ 2701-2713 (the "SCA"). *Id*. at ¶¶ 71-83. BMC moved to dismiss for lack of subject matter jurisdiction under Federal Rule of Civil Procedure ("FRCP") 12(b)(1) and failure to state a claim under FRCP 12(b)(6). Dkt. 123. Santos-Pagan opposed, Dkt. 126, and BMC replied, Dkt. 129. This case is before me by consent of the parties. Dkt. 79.

For the reasons set forth below, BMC's motion to dismiss is **GRANTED**.

BACKGROUND

BMC is a hospital in Bayamón, Puerto Rico. Dkt. 113 at ¶ 10. On May 21, 2019, BMC was subject to a cyberattack. *Id*. at ¶ 16. Records containing medical diagnoses, demographic information, financial information, dates of birth, and social security numbers of approximately 522,493 patients of BMC were implicated in the attack. *Id*. at ¶ 1; Dkt. 123-1 at 1. On July 19,

2019, BMC sent notices to the affected patients informing them of the incident. Dkt. 123-1 at 1. The notice stated that the patients' PHI and PII was temporarily locked through encryption, but that no data was irrevocably lost and there was no evidence suggesting any information was exfiltrated from the network. *Id*. at 1-2. Despite this, the notice provided steps that patients could undertake to protect themselves from any potential misuse of their information. *Id*. at 2. Santos-Pagan, a citizen of Puerto Rico, was a patient at BMC before the cyberattack. Dkt. 113 at ¶ 8. Following the cyberattack, Santos-Pagan discovered that a cellphone account was opened in her name with a company that she had never used. *Id*. at ¶ 9. The fraudulent account damaged her credit score, and she spent time and money (approximately $800) to repair it. *Id*. She continues to incur costs related to monitoring her credit for fraudulent charges. *Id*.

STANDARD OF REVIEW

BMC moved to dismiss for lack of subject matter jurisdiction under FRCP 12(b)(1) and for failure to state a claim under FRCP 12(b)(6). "Motions brought under Rule 12(b)(1) and Rule 12(b)(6) are subject to the same standard of review." *Hart v. Mazur*, 903 F. Supp. 277, 279 (D.R.I. 1995). "The party invoking federal jurisdiction has the burden of establishing that the court has subject matter jurisdiction over the case." *Amoche v. Guar. Tr. Life Ins. Co.*, 556 F.3d 41, 48 (1st Cir. 2009). When "confronted with motions to dismiss under both Rules 12(b)(1) and 12(b)(6), [courts] ordinarily ought to decide the former before broaching the latter." *Gonzalez v. Otero*, 172 F. Supp. 3d 477, 495 (D.P.R. 2016) (citation omitted). "After all, if the court lacks subject matter jurisdiction, assessment of the merits becomes a matter of purely academic interest." *Id*. (citation omitted). When evaluating a motion to dismiss under FRCP 12(b)(1), "courts construe the Complaint liberally and treat all well-pleaded facts as true, according the plaintiff[s] the benefit of

all reasonable inferences." *Rivera-Marrero v. Banco Popular de P.R.*, No. 22-1217 (ADC), 2023 U.S. Dist. LEXIS 57307, 2023 WL 2744683, at *6 (D.P.R. Mar. 31, 2023) (citation omitted).

"Courts also favorably construe a complaint when considering a Rule 12(b)(6) motion to dismiss for failure to state a claim upon which relief can be granted." *Id*. (citing *Rodríguez-Reyes v. Molina-Rodríguez*, 711 F.3d 49, 53 (1st Cir. 2013)). "While detailed factual allegations are not necessary to survive a motion to dismiss for failure to state a claim, a complaint nonetheless must contain more than a rote recital of the elements of a cause of action" and "must contain sufficient factual matter to state a claim to relief that is plausible on its face." *Id.* (citing *Ashcroft v. Iqbal*, 556 U.S. 662, 678-79, 129 S. Ct. 1937, 173 L. Ed. 2d 868 (2009)) (additional citations and internal quotation marks omitted). When performing this plausibility inquiry, the court must "separate factual allegations from conclusory ones and then evaluate whether the factual allegations support a 'reasonable inference that the defendant is liable for the misconduct alleged.'" *Conformis, Inc. v. Aetna, Inc.*, 58 F.4th 517, 528 (1st Cir. 2023) (*citing Iqbal*, 556 U.S. at 678, and *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570, 127 S. Ct. 1955, 167 L. Ed. 2d 929 (2007)). If the resulting factual allegations "are too meager, vague, or conclusory to remove the possibility of relief from the realm of mere conjecture, the complaint is open to dismissal." *S.E.C. v. Tambone*, 597 F.3d 436, 442 (1st Cir. 2010) (*en banc*). In sum, "[t]he relevant inquiry focuses on the reasonableness of the inference of liability that the plaintiff is asking the court to draw from the facts alleged in the complaint." *Ocasio-Hernandez v. Fortuño-Burset*, 640 F.3d 1, 13 (1st Cir. 2011).

DISCUSSION

BMC seeks dismissal of this action for a) lack of subject matter jurisdiction, and b) failure to state a claim upon which relief can be granted. Specifically, BMC argues that 1) there is no basis for federal court jurisdiction, 2) Santos-Pagan does not have Article III standing, and 3) her claims

fail on the merits. For the reasons set forth below, Santos-Pagan's complaint must be dismissed for lack of both federal jurisdiction and standing.

A. Federal Jurisdiction

Santos-Pagan posits two bases for federal court jurisdiction. First, she asserts federal question jurisdiction under 28 U.S.C. § 1331 via her federal SCA claim, which in turn provides supplemental jurisdiction over her Puerto Rico law claims arising out of "the same case or controversy." 28 U.S.C. § 1367(a). Alternatively, she asserts jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d) ("CAFA").

i. Stored Communications Act

The SCA provides a cause of action for "any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind." 18 U.S.C. § 2707(a). Santos-Pagan alleges that "[b]y failing to take reasonable steps to safeguard Plaintiff's and Class Member's PHI and PII while in electronic storage, BMC allowed unauthorized access to its electronic systems and knowingly divulged patient PHI and PII." Dkt. 113 at ¶ 76. In addition to disputing whether any PHI or PII was actually divulged, BMC argues that they did not have the requisite "knowing or intentional state of mind" for liability under the SCA. Dkt. 123 at 21.

Defendants are correct. Failure to take reasonable steps to safeguard PHI and PII does not meet the knowing state of mind requirement under the SCA, as has been recognized by several district courts before us. *See Rodriguez v. Mena Hosp. Comm'n*, No. 2:23-cv-20020F, 2023 U.S. Dist. LEXIS 196396, 2023 WL 7198441, at *42 (W.D. Ar. Nov. 1, 2023) ("Here, Plaintiffs allege Mena failed to take reasonable steps to safeguard Plaintiffs' PII. At least one district court has held nearly identical language does not state a claim under the SCA") (internal quotations and

alterations omitted); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2017 U.S. Dist. LEXIS 140212, 2017 WL 3727318, at *152 (N.D. Cal. Aug. 30, 2017) ("Plaintiffs allege only that Defendants failed to take commercially reasonable steps to safeguard Plaintiffs' communications. This allegation, without more, does not establish that Defendants divulged Plaintiffs' PII and did so with a knowing state of mind.") (internal quotations and alterations omitted). Santos-Pagan does not claim that BMC knowingly handed out patient PHI and PII without authorization. While she claims that BMC "intentionally did not take reasonable steps" and "willfully failed to put adequate safeguards in place," Dkt. 126 at 15, these phrasings are akin to claiming BMC knowingly behaved negligently, which does not meet the mental state requirement of the SCA. Therefore, Santos-Pagan's SCA claim is without merit and cannot be used to establish federal jurisdiction for her case.

ii. Class Action Fairness Act

Santos-Pagan's second argument for federal jurisdiction is through the CAFA, which provides jurisdiction for class actions in which 1) the amount in controversy exceeds $5,000,000, and 2) "minimal diversity" exists between the plaintiffs and defendants. 28 U.S.C. § 1332(d)(2).

With respect to the amount in controversy requirement, "[i]n suits initially filed in federal court, the amount specified by the plaintiff controls, as long as that amount is asserted in good faith." *Amoche*, 556 F.3d at 49 fn.3 (citation omitted). "Once the damages allegation is challenged, however, the party seeking to invoke jurisdiction has the burden of alleging with sufficient particularity facts indicating that it is not a legal certainty that the claim involves less than the jurisdictional amount." *Id*. (internal quotation marks omitted).[1]

[1] This standard applies for plaintiffs who bring their suit in federal court initially. A higher standard of proof (demonstrating a "reasonable probability" the amount in controversy requirement is exceeded) is required for defendants seeking to remove a class action from state court to federal court. *Amoche*, 556 F.3d at 50.

Santos-Pagan has met her burden with respect to the amount in controversy requirement. As the representative plaintiff, Santos-Pagan alleges that she was forced to spend $800 to repair her credit after the unauthorized cellphone account was set up in her name. Dkt. 113 at ¶ 9. She incurred additional costs in time and money to continue monitoring her credit, "the cost of which ranges from $100 to $300 annually," according to the complaint. *Id*. at ¶ 59. She also provides evidence that "particularly acute" exposures of medical information may cost a patient $20,000. *Id*. at ¶ 50. Given the potential size of the class (over 500,000 patients affected), damages of under $10 per class member would suffice to satisfy the $5 million amount in controversy requirement. Therefore, Santos-Pagan has shown that failure to reach the amount in controversy requirement is far from a legal certainty.

Establishing minimal diversity is another matter. Minimal diversity is present whenever one plaintiff is a citizen of a State (including Puerto Rico, *see* 28 U.S.C. § 1332(e)) different from any defendant. 28 U.S.C. § 1332(d)(2)(A). That plaintiff does not need to be a named plaintiff, nor does the class need to be certified. 28 U.S.C. § 1332(d)(1)(D). Courts take differing positions on whether a party needs to present an individual plaintiff who is diverse from the defendant to establish minimal diversity, or whether a "reasonable probability" that a class will contain a diverse member suffices. *Compare McMorris v. TJX Cos.*, 493 F. Supp. 2d 158, 164, fn. 2 (finding a "reasonable probability that one member of the McMorris class is domiciled in a state other than Massachusetts or Delaware, the two states in which TJX is domiciled," despite the named plaintiffs being domiciled in Massachusetts), *and Preaster v. Fulton Sav. Bank*, 5:22-cv-00342 (AMN/TWD), 2023 U.S. Dist. LEXIS 99908, 2023 WL 3847468, at *7-8 (N.D.N.Y. Mar. 21, 2023) (finding minimal diversity based on "reasonable probability that at least one class member is not a citizen of New York" despite named plaintiffs and defendant both being New York

citizens), *with Faris v. Petit Pot, Inc.*, No. 23-1955-JFW(PDx), 2023 U.S. Dist. LEXIS 145371, 2023 WL 6192703, at *3 (C.D. Cal. Aug. 18, 2023) ("[A] conclusory and prospective allegation that at least one unknown member of a nationwide class will result in minimal diversity is not sufficient to satisfy the pleading requirements for CAFA jurisdiction") (citation omitted), *and Canseven v. Just Pups, LLC*, No. 15-5633, 2015 U.S. Dist. LEXIS 123223, 2015 WL 5455869, at *4-5 (D.N.J. Sept. 16, 2015) ("Defendants' argument that there may be a member of the class who is not currently a New Jersey citizen is too speculative to create minimal diversity on its own.").

I find that Santos-Pagan has not met her burden to establish minimal diversity. I decline to find minimal diversity based on class definition alone – Santos-Pagan must show that there is at least one member of the putative class who is a citizen of a different state from the defendant. This she fails to do. Both Santos-Pagan and BMC appear to be citizens of Puerto Rico, and Santos-Pagan is the only class member whose citizenship is discussed in the complaint. Dkt. 113 at ¶¶ 8, 10; Dkt. 123 at 18. Asserting that the class is broadly defined to include "all United States citizens, not just Puerto Rican citizens," Dkt. 126 at 18, is not enough to satisfy her burden of showing minimal diversity.[2]

In the alternative, Santos-Pagan requests leave to perform jurisdictional discovery concerning the citizenship of potential class members and amend her complaint accordingly, claiming that this information is uniquely possessed by BMC. Dkt. 126 at 18. When jurisdiction is uncertain, courts in this circuit occasionally allow limited jurisdictional discovery. *See, e.g.*, *BRT Mgmt. LLC v. Malden Storage LLC*, 68 F.4th 691, 698-99 (1st Cir. 2023) (describing with approval

[2] In addition to contesting minimal diversity, BMC alleges that the CAFA "home state" exception bars jurisdiction. *See* Dkt. 129 at 10. The "home state" exception requires courts to decline jurisdiction if "two-thirds or more of the members of all proposed plaintiff classes in the aggregate, and the primary defendants, are citizens of the State in which the action was originally filed." 28 U.S.C. § 1332(d)(4)(B). Since Santos-Pagan fails to establish minimal diversity, I do not reach whether the home state exception applies, but note that as the party "seek[ing] to avail itself of [the] exception," BMC would bear the burden of proving its applicability. *McMorris*, 493 F. Supp. 2d at 165 (citing *Evans v. Walter Indus., Inc.*, 449 F.3d 1159, 1164 (11th Cir. 2006)).

case history where plaintiff was allowed limited jurisdictional discovery when "the information necessary to establish jurisdiction [was] uniquely in the possession of the would-be defendant."). However, as will be shown below, Santos-Pagan fails to establish standing for her claims. Had class citizenship been the only issue with respect to subject matter jurisdiction, limited jurisdictional discovery may have been appropriate. But here, it would ultimately serve no purpose. I therefore conclude that Santos-Pagan has not met her burden of showing minimal diversity and deny jurisdictional discovery on the question of class citizenship.

B. Standing

BMC's second challenge to this court's subject-matter jurisdiction is that Santos-Pagan does not have standing for her claims. Santos-Pagan presents a collection of arguments to establish standing – actual misuse based on the fraudulent cellphone account, unauthorized disclosure of PII/PHI, costs spent mitigating risks of identity theft, imminent risk of future harm, loss of benefit of the bargain, and diminished value of PII/PHI. Dkt. 126 at 10-14. BMC challenges the factual basis and legal sufficiency of these alleged injuries. Dkt. 123 at 11-16; Dkt. 129 at 4-6.

The standing requirement stems from Article III of the Constitution, which limits "[t]he judicial Power" to "Cases" and "Controversies." U.S. Const. art. III, § 2, cl. 1. "Federal courts are courts of limited jurisdiction and…because standing is a prerequisite to a federal court's subject matter jurisdiction, the absence of standing may be raised at any stage of a case." *Quintero v. Metro Santurce, Inc.*, No. 20-01075-WGY, 2021 U.S. Dist. LEXIS 237071, 2021 WL 5855752, at *8 (D.P.R. Dec. 9, 2021). "[P]laintiffs bear the burden of demonstrating that they have standing." *Webb v. Injured Workers Pharm.*, 72 F.4th 365, 371 (1st Cir. 2023). To establish standing, "a plaintiff must show (i) that [she] suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury

would likely be redressed by judicial relief." *TransUnion LLC v. Ramirez*, 594 U.S. 413, 423, 141 S. Ct. 2190, 2203 (2021). At the pleading stage, "the party must clearly allege facts demonstrating each element of the standing inquiry." *Rivera-Marrero*, 2023 U.S. Dist. LEXIS 57307 at *12 (citation omitted). Where no class is yet certified, the court "evaluate[s] only whether the [named] plaintiff[s have] constitutional [] standing to pursue the action." *Katz v. Pershing, LLC*, 672 F.3d 64, 71 (1st Cir. 2012).

The way in which a cyberattack is performed, and the ends pursued by the hackers, influence whether class action plaintiffs will have standing. In many cases, hackers will obtain access to confidential data and copy it outside of the victim's computer system ("exfiltration"). Exfiltrated data can be used to commit crimes like identity theft, where a criminal pretends to be the person whose information was stolen for monetary gain. *See, e.g.*, *Webb.*, 72 F.4th at 369-70 (defendant pharma company was subject to a cyberattack, with hackers stealing PII and using it to file a fraudulent tax return in plaintiff's name). Another type of cyberattack, so-called "ransomware attacks," are performed by encrypting data on a victim's computer system, blocking their access and demanding a ransom payment in exchange for unlocking the data. *See Quintero*, 2021 U.S. Dist. LEXIS 237071 at *2 fn. 2 (defining and describing ransomware attacks). In "pure" ransomware attacks, no data will be exfiltrated and the sole intent of the hackers is to obtain the ransom payment. *Id*. at *7 ("[A] pure ransomware attack [is] an attack that holds data hostage but does not steal it."). Alternatively, hackers performing a ransomware attack may exfiltrate the data and threaten to publish it to extort a higher ransom payment. *See Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 150 (3d Cir. 2022) (cyberattack class action in which hackers stole sensitive patient information from a pharma company, then installed encrypting malware on the company's server,

withholding access to the data and threatening to publish the data on the dark web unless the company paid the ransom).

Numerous courts in this circuit have analyzed standing for damages in the context of cyberattack class actions. In *Quintero v. Metro Santurce, Inc.*, the defendant hospital was subject to a "pure" ransomware attack affecting the PHI and PII of its patients. The court found that the plaintiff failed to establish standing since there was no evidence that patient data was exfiltrated and misused. 2021 U.S. Dist. LEXIS 237071 at *17 ("That argument – access by encryption equals acquisition and misuse – is a bridge too far, mere speculation, and is not in accord with the modern trend in this area of the law."). The court based its decision on the fact that "the complaint fail[ed] sufficiently to allege motive other than a garden-variety ransomware attack" and that "the complaint does not allege the hackers intended to steal and sell information." *Id*. at *13.

On similar facts, *Rivera-Marrero v. Banco Popular de P.R.* addressed claims of standing based on "injur[y] due to the increased risk of future harm from the potential misuse of [plaintiff's] PII," along with incurrence of mitigation costs, diminution in PII value, lost time, annoyance, loss of benefit of the bargain, and anxiety. 2023 U.S. Dist. LEXIS 57307 at *35. In this case, the plaintiff alleged that her PII was exfiltrated by the hackers. *Id*. at *24. However, the court concluded that, without "allegation of any actual identity theft or misuse of her PII," the plaintiff's claimed injuries were "too speculative and abstract to be considered injuries in fact for standing purposes." *Id*. at *29, 35-36.

By contrast, in *Webb v. Injured Workers Pharm., LLC*, the First Circuit found standing for a class action plaintiff who provided evidence that her data was exfiltrated and used for identity theft. 72 F.4th at 372-77. In *Webb*, the defendant pharma company suffered a cyberattack in which hackers infiltrated their patient record systems and stole PII, including patient names and social

security numbers. *Id*. at 369-70. The company did not discover the breach until nearly four months after it occurred. *Id*. Following the attack, a fraudulent tax return was filed in the plaintiff's name. *Id*. The First Circuit held that "plausible allegations of actual misuse of [plaintiff's] stolen PII to file a fraudulent tax return suffice to state a concrete injury under Article III." *Id*. at 373. The court found that the plaintiff had "plausibly allege[d] a connection between the data breach and the filing of the false tax return," noting that there was "an obvious temporal connection between the filing of the false tax return and the timing of the data breach" and that the plaintiff was "very careful about sharing her PII, ha[d] never knowingly transmitted unencrypted PII over the internet or any other unsecured source, and store[d] documents containing her PII in a secure location." *Id*. at 373-74. This created an "obvious inference…that the criminal or criminals who filed the false tax return obtained [plaintiff's] PII from the [] data breach, not from some other source." *Id*. The court also found standing for the other class members despite the fact they did not provide evidence that their PII was used for identity theft. *Id*. at 374-77. Since one class member was subject to identity theft traceable to the data breach, the risk of future identity theft for each other class member was considered sufficiently "imminent" to confer standing. *Id*.

Based on the above precedents, Santos-Pagan's standing hinges on showing a "plausible allegation[] of actual misuse" tied to the BMC cyberattack. *Webb*, 72 F.4th at 373. To this end, she claims a fraudulent cellphone account was set up in her name, damaging her credit score. She claims that the service provider was one she never used and that she was forced to spend $800 to repair her damaged credit. *See supra* p. 2. According to Santos-Pagan, this shows patient data was exfiltrated in the BMC cyberattack and used for identity theft in at least one case, rendering the threat of future identity theft imminent. Dkt. 126 at 10-13.

BMC challenges these claims. First, they argue that Santos-Pagan's story of the fraudulent cellphone account should be struck from the record and disregarded for failure to meet FRCP 9(b)'s heightened pleading requirement for averments of fraud. Dkt. 123 at 16-17. FRCP 9(b) states that "[i]n alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake." "Particularity" means that a plaintiff must provide details such as time, place, and content of the fraudulent acts. *See Ahmed v. Rosenblatt*, 118 F.3d 886, 889 (1st Cir. 1997) ("[A] pleader must state the time, place, and content of the alleged mail and wire communications perpetrating [the] fraud."). However, BMC's invocation of FRCP 9(b) is misplaced. Since Santos-Pagan is not alleging that BMC committed fraud, but rather, that fraud was committed by a third party who accessed her information, FRCP 9(b)'s particularity requirement does not apply. *See* 5A Charles Alan Wright & Arthur R. Miller, *Federal Practice and Procedure* § 1297 (4th ed. 2018) ("[T]he reasons for the particularity rule are not present when the fraud alleged is that of someone who is not a party to the action, and it has been held that in such a case the circumstances of the fraud or mistake need not be pleaded by the plaintiff with any special degree of particularity"); *Nat'l Steel Corp. v. Maryland Cas. Co.*, 18 F.R.D. 166, 168 (W.D. Pa. 1955); *Fed. Deposit Ins. Corp. v. Fidelity & Deposit Co.*, 118 F.R.D. 435, 436 (M.D. La. 1988). Therefore, FRCP 9(b) does not provide a reason to strike Santos-Pagan's identity theft allegation.

BMC's second argument is that Santos-Pagan's identity theft allegation is not traceable to the cyberattack. BMC claims Santos-Pagan's allegation is "too attenuated, distant and remote and the [complaint] lacks sufficient allegations for a court to plausibly find causality or traceability to BMC." Dkt. 123 at 13. BMC attests that there is no evidence that data was exfiltrated or used to commit identity theft, noting they were subject to a ransomware attack, the aim of which is "to limit the data holder's access to its own data in order to extort payment" rather than to use the PII

for identity theft. *Id*. at 3; *see also In re Practicefirst Data Breach Litig.*, No. 1:21-CV-00790(JLS/MJR), 2022 U.S. Dist. LEXIS 19272, 2022 WL 354544, at *16 (W.D.N.Y. Feb. 1, 2022) ("[T]he primary purpose of a ransomware attack is the exchange of money for access to data, not identity theft.").

"The Article III traceability inquiry is not as strict as the tort causation standard, demanding only that the data breach plausibly caused Plaintiff's injury." *Capiau v. Ascendum Mach., Inc.*, No. 3:24-cv-00142-MOC-SCR, 2024 U.S. Dist. LEXIS 142393, 2024 WL 3747191, at *19 (W.D.N.C. Aug. 8, 2024); *see also Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 134 S. Ct. 1377, 572 U.S. 118, 134 fn. 6 (2014) ("Proximate causation is not a requirement of Article III standing."). A competing potential cause, such as a different data breach, does not render an injury un-traceable. *See In re Zappos.com, Inc.*, 888 F.3d 1020, 1029 (9th Cir. 2018) (such an argument is "less about standing and more about the merits of causation and damages."). However, "the mere fact that [plaintiffs] experienced misuse of their PII…is insufficient to show that the misuse of their PII is fairly traceable to the [defendant's] data breach." *Williams v. Bienville Orthopaedic Specialists, LLC*, No. 1:23CV232-LG-MTP, 2024 U.S. Dist. LEXIS 107885, at *26 (S.D. Miss. Jun 18, 2024). An important component of traceability in the cyberattack context is whether the information used in the identity theft matches the information that the defendant had on file. *See Masterson v. IMA Fin. Grp., Inc.*, No. 2:23-cv-02223-HLT-ADM, 2023 U.S. Dist. LEXIS 222701, 2023 WL 8647157, at *10 (D. Kan. Dec. 14, 2023) (rejecting standing on traceability noting that "there are no allegations that [defendant] had the information [plaintiffs] claim was misused."). Logically, if the identity theft required information that the defendant did not have on file, it cannot be fairly traced to the cyberattack. By contrast, a strong argument for traceability exists if the

defendant had on file confidential information which was necessary to commit the act of identity theft in question.

I find that Santos-Pagan has not met her burden to show that the fraudulent cellphone account is traceable to BMC's cyberattack. Beyond the fact that the account was set up at some point after the cyberattack, she does not allege any evidence suggestive of a link between the two events. Unlike the plaintiff in *Webb*, she does not provide a specific timeframe for when the fraudulent account was set up that might suggest an "obvious temporal connection" with the cyberattack. *Webb*, 72 F.4th at 374. Nor does she attest that she was "careful about sharing her PII," "never knowingly transmitted unencrypted PII over the internet or any other unsecured source," or "store[d] documents containing her PII in a secure location," which would support an "inference…that the criminal or criminals who [set up the cellphone account] obtained [her] PII from the [BMC] data breach, not from some other source." *Id*. Critically, Santos-Pagan did not aver that setting up the fraudulent cellphone account would have required the same information BMC had in her file. For instance, she might have demonstrated that setting up a cellphone account with the particular service provider would have required her social security number, which BMC had on file. Since social security numbers are unique to each individual and generally safeguarded, this would have provided grounds to infer that whoever set up the fraudulent cellphone account plausibly did so with information obtained in the cyberattack. Such was the case in *Webb* – filing a tax return requires an individual's social security number, which the defendant pharma company had on file. *Id*. at 369.

The burden for establishing traceability is "relatively modest at this stage of the litigation." *Alleruzo v. SuperValu, Inc.*, 870 F.3d 763, 772 (8th Cir. 2017) (citation omitted). However, Santos-Pagan has not provided any evidence to connect the alleged identity theft to BMC's cyberattack.

Consequently, she has failed to establish Article III standing. This court is thus without jurisdiction to hear her case.

CONCLUSION

For the foregoing reasons, BMC's motion to dismiss is **GRANTED.** The claims under the SCA are dismissed with prejudice, and the claims arising under Puerto Rico law are dismissed without prejudice.

IT IS SO ORDERED.

In San Juan, Puerto Rico, this 30th day of September, 2024.

/s/ Bruce J. McGiverin
BRUCE J. MCGIVERIN
United States Magistrate Judge